Daily Open Source Infrastructure Report
13 November 2015

Top Stories

- Indictments against 44 people and 9 companies were unsealed November 10 detailing an alleged scheme to steal and resell approximately $34 million worth of oil that was never delivered to various businesses in New York. – *New York Times* (See item 2)
- Volkswagen announced November 10 that production of diesel-powered 2016 Passat TDI sedans was temporarily stopped at its Chattanooga, Tennessee plant. – *Chattanooga Times Free Press* (See item 3)
- Chipotle Mexican Grill, Inc., re-opened 43 restaurants in Oregon and Washington November 12 after they underwent thorough cleaning following an E. coli outbreak. – *Associated Press* (See item 12)
- A grand jury in Waco, Texas, indicted 106 out of 177 bikers November 10 who were arrested for engaging in organized criminal activity following a May 17 shootout that killed 9 people and injured 20 others. – *Associated Press* (See item 25)

Fast Jump Menu

Energy Sector

1. *November 12, Pottsville Republican & Herald* – (Pennsylvania) **Police: Employee stole $400K from Gilbert Coal Co. over 8 years.** A Frackville man and former employee of Gilbertson Coal Co., was charged by authorities for allegedly stealing over $400,000 from the company between January 2006 and December 2014 by various means including check fraud and forgery.
   Source: http://republicanherald.com/news/police-employee-stole-400k-from-gilberton-coal-co-over-8-years-1.1970576

2. *November 10, New York Times* – (New York) **Prosecutors allege persistent heating oil fraud in New York City.** The Manhattan district attorney's office unsealed indictments November 10 against 44 people and 9 companies for allegedly stealing and reselling approximately $34 million worth of oil that was never delivered to homeless shelters, hospitals, courthouses, police stations, and prison buildings on Rikers Island. The investigation uncovered 48 seized trucks that were rigged to deprive customers of their fuel, among several other fraudulent activities.
   Source: http://www.nytimes.com/2015/11/11/nyregion/11-indictments-detail-widespread-fraud-in-heating-oil-industry-of-new-york-city.html

For another story, see item **10**

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

3. *November 11, Chattanooga Times Free Press*– (Tennessee) **VW plants stops production of diesel Passats while awaiting emissions fix.** Volkswagen announced November 10 that production of diesel-powered 2016 Passat TDI sedans were temporarily ceased at its Chattanooga plant while it awaits a fix to the vehicles containing illegal software that masked their emissions.
   Source:
   http://www.timesfreepress.com/news/business/aroundregion/story/2015/nov/11/vw-stops-chattanoogpassproductiwhile-awaiting/335072/

4. *November 11, Plattsburgh Press-Republican* – (New York) **Fire at Swarovski evacuates employees.** Operations at the Swarovski Lighting Ltd. plant in Plattsburgh were ceased indefinitely due to a November 11 fire that started in a blower unit that exhausts metal filings out of a sanding and grinding booth. Employees were evacuated and the total amount of damages is being assessed.
   Source: http://www.pressrepublican.com/news/fire-at-swarovski-plant-

doused/article_c4a4e666-88a2-11e5-92bb-33416ec63e0b.html

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

5. *November 12, Securityweek* – (International) **"Cherry Picker" PoS malware cleans up after itself.** Researchers from Trustwave discovered that a point-of-sale (PoS) malware dubbed "Cherry Picker" relies on a new memory scraping algorithm using a file infector for persistence that removes all traces of the infection from the system with updated versions of sr.exe and srf.exe, which has been used to install the malware and inject a data definition language (DLL) into processes. The latest version of the malware relies on an application programming interface (API) called "QueryWorkingSet" to scrape the memory and harvest the data.
Source: http://www.securityweek.com/cherry-picker-pos-malware-cleans-after-itself

Transportation Systems Sector

6. *November 11, ABC News* – (Alabama) **Plane makes emergency landing after passenger spots fuel leaking from wing.** An ExpressJet Airlines flight headed to Dallas-Fort Worth diverted to Huntsville, Alabama, November 11 after a passenger noticed fuel leaking out of the wing and alerted a flight attendant. The plane landed safely and the airline worked to accommodate the 41 passengers on a replacement aircraft.
Source: http://abcnews.go.com/US/plane-makes-emergency-landing-passenger-spots-fuel-leaking/story?id=35134132

7. *November 11, CNN* – (Ohio) **Akron plane crash: Shock, horror after plane slams into apartment building.** The Federal Aviation Administration and the U.S. National Transportation Board reported November 11 that a small Hawker 700 plane crashed into an unoccupied apartment building in Akron, Ohio, killing all 9 people on board and causing extensive damage to the building November 10. The occupants of the apartment building as well as the occupants of eight apartment units in two surrounding buildings were displaced by the incident.
Source: http://www.cnn.com/2015/11/11/us/akron-ohio-plane-crash/

8. *November 11, Dickson Herald* – (Tennessee) **Broken pole, down line causes Dickson traffic gridlock.** Highway 46 South in Dickson was reduced to 1 lane for nearly 5 hours November 10 while crews worked to repair a downed power pole and an attached cable that fell across the highway after a Stansell Electric truck working on the highway snagged a communication cable that was attached to a Dickson Electric System main line. Officials turned off power in the area while working to repair the damage.
Source: http://www.tennessean.com/story/news/local/dickson/2015/11/11/broken-pole-down-line-causes-dickson-traffic-gridlock/75574904/

9. *November 11, WITI 6 Milwaukee* – (Wisconsin) **Canadian Pacific: Another derailment near scene of Sunday's train derailment in Watertown.** A Canadian Pacific spokesperson reported November 11 that 5 rail cars derailed as they were being moved in Watertown, 4 days after 13 cars from Canadian Pacific train carrying Bakken crude oil derailed November 8. The cars were re-railed within 2 hours and an investigation into the derailment is ongoing.
Source: http://fox6now.com/2015/11/11/canadian-pacific-another-derailment-near-scene-of-sundays-train-derailment-in-watertown/

10. *November 10, Chicago Tribune* – (Illinois) **Feds reject call for tougher fire-resistance for crude oil tank cars.** The U.S. Department of Transportation announced November 10 that it is upholding its decision issued in the spring of 2014 to require new and retrofitted tank cars to be required to withstand being engulfed in a pool of burning liquid for 100 minutes without exploding, and rejected a call to toughen the fire-resistance of railroad tank cars that carry highly flammable crude oil. The department stated that 100 minutes was adequate time for first responders to assess the accident and evacuate the area.
Source: http://www.chicagotribune.com/news/ct-crude-oil-tank-care-met-20151110-story.html

11. *November 10, Federal Aviation Administration* – (California) **FAA proposes $68,000 civil penalty against Unical Aviation.** The Federal Aviation Administration (FAA) proposed November 10 a $68,000 civil penalty against the City of Industry, California-based Unical Aviation Inc., for allegedly offering undeclared hazardous material shipments to FedEx for transport by air to Lenexa, Kansas July 21. The FAA alleges that the shipments were not accompanied by shipping papers and were not properly packaged, marked, or labeled as containing hazardous materials.
Source: https://www.faa.gov/news/press_releases/news_story.cfm?newsId=19714

Food and Agriculture Sector

12. *November 12, Associated Press* – (Oregon; Washington) **Chipotle reopening all Northwest locations after E. coli outbreak.** Chipotle Mexican Grill, Inc., re-opened 43 restaurants in Oregon and Washington November 12 after they underwent thorough cleaning, and the company adopted some new protocols for washing fresh produce following an E. coli outbreak that sickened nearly 45 people. The cause of the outbreak remains under investigation and Chipotle announced that it did not find any food contaminated by E. coli following testing.
Source: http://registerguard.com/rg/business/33707286-63/chipotle-reopening-all-northwest-locations-after-e.-coli-outbreak.csp

13. *November 10, U.S. Food and Drug Administration* – (Oregon) **Old Oregon Smokehouse is issuing a voluntary recall Canned Albacore Tuna because of a possible health risk.** Oregon-based Old Oregon Smokehouse issued a voluntary recall November 10 for all canned Albacore Tuna products packaged in 6 ounce cans due to potential Clostridium botulinum contamination after a routine inspection of a Skipanon Brand Seafoods LLC facility revealed that the products may be contaminated with the

bacterium due to under processing. Products were sold to consumers in retail stores in Tillamook and Rockaway, Oregon.
Source: http://www.fda.gov/Safety/Recalls/ucm472252.htm

14. *November 9, U.S. Department of Labor* – (Texas) **After amputation at Austin manufacturing plant, OSHA cites employer and temp agency for safety violations.** The U.S. Department of Labor issued one willful safety violation and one serious violation to Genesis Today Inc., a health food manufacturer, and Texas Management Division Inc., a temporary employment agency that provides workers to the company, for failing to provide safety guards for dangerous machines November 9 following an incident where a worker's hand was caught in a machine and amputated. Genesis Today was issued a $56,000 fine while Texas Management Division was issued a $7,000 fine.
Source: https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=29034

Water and Wastewater Systems Sector

15. *November 11, WFAA 8 Dallas* – (Texas) **Some Plano water affected by sewer overflow.** Officials reported November 11 that an estimated 797,000 gallons of wastewater overflowed into Plano storm drains that emptied into Spring Creek due to a break in a sewage line November 10. The spill was contained and residents were advised to avoid waste material, soil, and water in the area near the spill.
Source: http://www.wfaa.com/story/news/local/collin-county/2015/11/11/some-plano-water-affected-sewer-overflow/75607106/

Healthcare and Public Health Sector

16. *November 11, Harrisburg Patriot-News* – (Pennsylvania) **Another York Hospital patient with rare open heart surgery-related infection dies.** WellSpan Health announced November 11 that a fifth patient died due to complications from potential exposure to nontuberculous mycobacteria during open-heart surgery at York Hospital in Pennsylvania. The infection has been linked to heater-cooler devices that are used during surgeries, prompting the hospital to sterilize and clean the units.
Source: http://www.pennlive.com/news/2015/11/ntm_hershey_heater-coolers.html

17. *November 10, KNSD 39 San Diego* – (California) **8 doctors, associates charged in bribery scheme involving worker's comp charges.** The U.S. attorney's office announced November 10 that 6 corporations and 8 defendants were charged in an alleged southern California bribery scheme that involved $25 million in improper worker's compensation charges after an investigation found that the medical professionals and associates were receiving kickbacks for patient referrals, in addition to receiving kickbacks for referring patients to specialized treatments.
Source: http://www.nbcsandiego.com/news/local/Officials-Announce-Major-Healthcare-Fraud-Case-345022712.html

For another story, see item 2

Government Facilities Sector

See item 2

Emergency Services Sector

See item 2

Information Technology Sector

18. *November 12, Securityweek* – (International) **Microsoft reissues security update due to Outlook crash.** Microsoft reissued a security patch updating its KB3097877 software on Windows 7 and some versions of its KB3105213 update on Windows 10 after customer complaints revealed that the software update had an issue with its Outlook 2010 and 2013 versions which caused crashes for consumers viewing HyperText Markup Language (HTML) emails.
Source: http://www.securityweek.com/microsoft-reissues-security-update-due-outlook-crash

19. *November 11, Securityweek* – (International) **Attackers abuse security products to install "Bookworm" trojan.** Researchers from Palo Alto Networks discovered a new trojan dubbed "Bookworm" which captures keystrokes and steals the content of a clipboard, as well as load additional modules from its command and control (C&C) server to expand its abilities by using a Smart Installer Maker tool to disguise the malware as a self-extracting RAR archive, or a Flash slideshow/installer, to write a executable data definition language (DDL) file named "Loader.ddl," and a file named "readme.txt," to the victims' system.
Source: http://www.securityweek.com/attackers-abuse-security-products-install-bookworm-trojan

20. *November 10, Softpedia* – (International) **Here's the list of all security bugs that Adobe fixed in Flash 19.0.0.245.** Adobe released patches for 17 critical bugs in its Flash Player 19.0.0.245 for Windows and Apple Mac, Flash Player 11.2.202.548 for Linux systems, as well as Adobe AIR that patched vulnerabilities including a type confusion flaw, and a security bypass vulnerability that allows attackers to write data to the target's file system with the user's permission.
Source: http://news.softpedia.com/news/here-s-the-list-of-all-security-bugs-that-adobe-fixed-in-flash-19-0-0-245-495990.shtml

For another story, see item 5

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: http://www.us-cert.gov

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: http://www.it-isac.org

Communications Sector

21. *November 11, Alpine Avalanche* – (Texas) **Telephone service disrupted.** AT&T customers located in 6 counties across southwest Texas experienced landline and some cellphone and Internet outages for about 8 hours November 10 due to a line break.
Source: http://www.alpineavalanche.com/news/article_28099a60-88dc-11e5-b042-bfdaaa41d229.html

Commercial Facilities Sector

22. *November 12, WFIE 14 Evansville* – (Kentucky) **New details released on Madisonville Walmart gas leak.** A Madisonville, Kentucky Walmart was evacuated and closed for nearly 6 hours November 11 after a drilling crew ruptured a methane gas pocket near the building. The store reopened November 12 and officials reported that there was no threat to the public.
Source: http://www.14news.com/story/30494319/madisonville-walmart-evacuated-due-to-gas-leak

23. *November 12, WVIT 30 New Britain* – (Connecticut) **Crews continue to fight Glastonbury factory fire as concerns over toxic gases arise.** Crews continued to battle a fire at the Preferred Display cosmetic display manufacturing plant in Glastonbury November 12 that prompted the evacuation of 75 employees. Officials urged residents to avoid areas where smoke was circulating due to concerns that the burning plastic could break down into toxic gases.
Source: http://www.nbcconnecticut.com/news/local/NATL-HAR-Glastonbury-Factory-Fire-Prompts-Concerns-of-Toxic-Gases-346611932.html

24. *November 11, KTLA 5 Los Angeles* – (California) **Bomb threat forces temporary evacuation of Target store in Manhattan Beach.** The Manhattan Beach Police Department reported November 11 that a Target store was evacuated and closed for approximately 4 hours while authorities searched for a suspicious device after a store employee received a phoned bomb threat. The store was deemed safe and no devices were found.
Source: http://ktla.com/2015/11/11/bomb-threat-forces-evacuation-of-target-store-in-manhattan-beach/

25. *November 11, Associated Press* – (Texas) **Grand jury indicts 106 bikers in Waco shootout with police.** A grand jury in Waco, Texas, indicted 106 out of 177 bikers November 10 who were arrested for engaging in organized criminal activity following a May 17 shootout with police at the Twin Peaks restaurant that killed 9 people and

injured 20 others after the Bandidos and the Cossacks motorcycle clubs had an alleged confrontation.
Source: http://www.foxnews.com/us/2015/11/11/grand-jury-indicts-106-bikers-in-waco-shootout-with-police/

For another story, see item 7

Dams Sector

Nothing to report

Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: http://www.dhs.gov/IPDailyReport

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703) 942-8590
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer